Listing of Claims:

1. (Currently Amended) A certification method using a public key certification authority ~~(30)~~ and involving ~~at least one~~ a mobile terminal ~~(10) able~~ identified on a mobile telecommunications network, the mobile terminal being configured to receive messages encrypted by ~~that~~ a public certification key, ~~wherein~~ the method ~~comprises~~ comprising:

generating, at the ~~step of the~~ mobile terminal, ~~(10) generating~~ the public certification key;

acquiring, at ~~the step of~~ a telecommunications network entity of the mobile telecommunications network, ~~(20) acquiring~~ said public certification key from the mobile terminal via ~~(10) by means of~~ a network call on the mobile telecommunications network;

authenticating, at ~~the step of~~ the telecommunications network entity, ~~authenticating~~ the mobile terminal ~~(10)~~ by a party authentication process ~~used in relation to~~ which is implemented in a standard telephone call on the mobile telecommunications network; and

~~the step of~~ supplying ~~the certification authority (30) with~~ the public certification key and ~~the~~ an associated authentication result to the public key certification authority. ~~of the authentication process~~[[.]]

2. (Currently Amended) [[A]] The method according to claim 1, wherein the step of authenticating the mobile terminal ~~(10)~~ includes sending, from the mobile terminal, ~~(10) sending~~ a calculation result involving a confidential key stored in the mobile terminal and comparing, at the ~~step of the~~ telecommunications network entity, ~~(20) comparing~~ the calculation result with an

expected result also calculated by the telecommunications network entity ~~(20) using~~ based on the ~~same~~ confidential key, a positive comparison result being ~~interpreted as~~ an identification of the mobile terminal.

3. (Currently Amended) [[A]] The method according to claim 2, further comprising the step of:

sending ~~the network entity sending~~ random data from the telecommunications network entity to the mobile terminal; and ~~the step of~~

calculating, at the mobile terminal, ~~calculating~~ the random data sent by the telecommunications network entity, the ~~step of~~ calculation by the telecommunications network entity also involving said random data ~~with a view to~~ based on said comparison of the calculated results.

4. (Currently Amended) [[A]] The method according to claim 1, further comprising the step of:

generating, at the mobile terminal, ~~(10) generating~~[[,]] in addition to the public certification key, a confidential key ~~held~~ stored in memory in the mobile terminal ~~(10)~~ and used to decrypt received messages that were encrypted with the public certification key.

5. (Currently Amended) [[A]] The method according to claim 4, wherein the mobile terminal is ~~adapted~~ configured to send messages and to append to ~~them~~ said messages an authentication signature produced using the confidential key ~~that it~~ previously generated ~~itself~~ in

the mobile terminal.

6. (Currently Amended) [[A]] The method according to claim 1, further comprising the step of:

sending ~~the network entity (20) sending~~ the public certification key from the telecommunications network entity to the public key certification authority ~~(30)~~ via a channel that is secured against unauthorized reading.

7. (Currently Amended) [[A]] The method according to claim 1, further comprising the ~~step~~ steps of:

utilizing, at the mobile terminal, ~~(10) using~~ an authentication key of the mobile terminal ~~(10)~~ usually employed in relation to telephone calls;[[,]]

generating, at the mobile terminal, an encryption key;[[,]]

encrypting, at the mobile terminal, messages ~~using that~~ using the generated encryption key; and

sending said encrypted messages.

8. (Currently Amended) A mobile telecommunications system comprising:

~~at least one~~ a mobile terminal ~~(10)~~ identified on a mobile telecommunications network;

~~one~~ a telecommunications network entity of the mobile telecommunications system ~~(20)~~;

~~means in the mobile terminal (10) for generating a public key);~~

means in the telecommunications network entity ~~(20)~~ for acquiring ~~said~~ a

public certification key generated by ~~from~~ the mobile terminal ~~(10) by means of~~ via a network call on the mobile telecommunications network;

means for authenticating the mobile terminal ~~by means of~~ via an authentication process ~~used in relation to~~ which is implemented in a standard telephone call on the mobile telecommunications network;

a public key certification authority; and

means for supplying the certification authority with the public certification key generated by the mobile terminal and ~~the~~ an associated authentication result. ~~of the authentication process~~[[.]]

9. (Current Amended) A mobile telecommunications terminal identified on a mobile communications network, ~~(10)~~ comprising:

~~means for producing at least one key for decrypting messages received by the terminal; and~~

means for sending ~~said~~ a key produced by the mobile terminal to a public key certification authority ~~(30) by means of~~ by a network call via a telecommunications ~~telephone~~ network entity of the mobile telecommunications network ~~(20) so~~ such that said key produced by the mobile terminal becomes a public certification key which is used for encrypting messages to be received by the mobile terminal; and

means for storing the key produced by the mobile terminal.